You won't believe

how SSL/TLS certificates are advertised on the dark web!

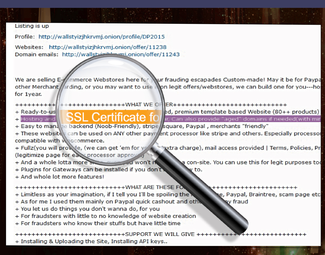
Why are TLS certificates attractive to attackers?

Fraudulent TLS certificates engender a false sense of trust that is ideal for disguising cybercriminal activity.
This makes TLS certificates a thriving commodity on the dark web.

Recent dark web research has uncovered a variety of advertisements for fraudulent TLS certificate services:

Trusted e-commerce stores

- Promotes "trustworthy" e-commerce stores designed to support fraudulent activity
- Offers commodities such as malware, security vulnerabilities and exploits
- Bonus add-on: stolen accounts and credit card credentials

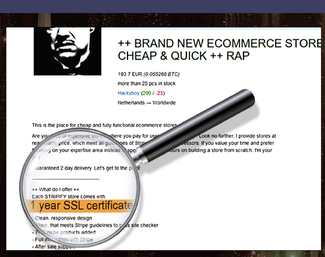


Fraudulent websites for novices

- Provides a detailed list of available fraudulent services
- Specifically targets "fraudsters" with little or no knowledge of website creation

Aged domains for sale

- Highlights SSL certificates and aged domains as key services
- Advertises price for a fraud-ready website at less than €200



Bargain SSL strip tool

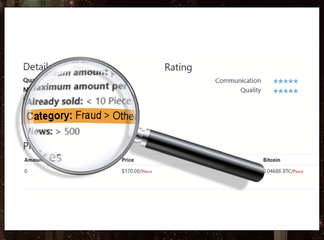
- Advertises an SSL Strip tool for less than $5
- SSL stripping exposes users to eavesdropping and data manipulation

Complete fake company ID

- Offers full support in establishing a company's identity in the U.K. for $150
- Includes the required legal documentation
- Upsell: vendor provides a physical address for an extra $100

Happy dark web customers

- Note the customer service ratings for this vendor!



What should you do?

Protect your machine identities.

They are incredibly valuable—to your organization as well as cybercriminals.
Here are some tips to help you protect them:

Get complete visibility.
Know how many certificates you have and who owns them

Apply global intelligence.
Continually monitor certificate health across your organization.

Automate your certificate lifecycles.
Use lightning-fast automation to change out weak machine identities.

How bad is it?

Machine identities are being weaponized and sold as commodities to cybercriminals every hour of every day.

Learn more about how cybercriminals are selling them.

Download the full study

Credits:

To shine a light on the availability of SSL/TLS certificates on the dark web, the Evidence-Based Cybersecurity Research Group at the Andrew Young School of Policy Studies at Georgia State University and the University of Surrey spearheaded a research program, sponsored by Venafi.

The research explored online markets and hacker forums that were active on the Tor network, I2P and Freenet and collected data from October 2018 to January 2019.

Georgia State University | Andrew Young School of Policy Studies

Venafi

Learn more about how you can proactively protect all your machine identities at **venafi.com**